The family of ternary cyclotomic polynomials with one free prime

Yves Gallot, Pieter Moree and Robert Wilms

Abstract

A cyclotomic polynomial $\Phi_n(x)$ is said to be ternary if $n = pqr$ with p, q and r distinct odd primes. Ternary cyclotomic polynomials are the simplest ones for which the behaviour of the coefficients is not completely understood. Here we establish some results and formulate some conjectures regarding the coefficients appearing in the polynomial family $\Phi_{pqr}(x)$ with $p < q < r$, p and q fixed and r a free prime.

1 Introduction

The n-th cyclotomic polynomial $\Phi_n(x)$ is defined by

$$\Phi_n(x) = \prod_{\substack{1\le j\le n \\ (j,n)=1}} (x - \zeta_n^j) = \sum_{k=0}^{\infty} a_n(k)x^k,$$

with ζ_n a n-th primitive root of unity (one can take $\zeta_n = e^{2\pi i/n}$). It has degree $\varphi(n)$, with φ Euler's totient function. We write $A(n) = \max\{|a_n(k)| : k \ge 0\}$, and this quantity is called the height of $\Phi_n(x)$. It is easy to see that $A(n) = A(N)$, with $N = \prod_{p|n,\ p>2} p$ the odd squarefree kernel. In deriving this, one uses the observation that if n is odd, then $A(2n) = A(n)$. If n has at most two distinct odd prime factors, then $A(n) = 1$. If $A(n) > 1$, then we necessarily must have that n has at least three distinct odd prime factors. In particular for $n < 105 = 3\cdot 5\cdot 7$ we have $A(n) = 1$. It turns out that $A(105) = 2$ with $a_{105}(7) = -2$. Thus the easiest case where we can expect non-trivial behaviour of the coefficients of $\Phi_n(x)$ is the ternary case, where $n = pqr$, with $2 < p < q < r$ odd primes. In this paper we are concerned with the family of ternary cyclotomic polynomials

$$\{\Phi_{pqr}(x) | r > q\}, \tag{1}$$

where $2 < p < q$ are fixed primes and r is a 'free prime'. Up to now in the literature the above family was considered, but with also q free. The maximum coefficient (in absolute value) that occurs in that family will be denoted by

MSC2000. 11B83, 11C08
Keywords: ternary cyclotomic polynomial, coefficient

$M(p)$, thus $M(p) = \max\{A(pqr) : p < q < r\}$, with $p > 2$ fixed. Similarly we define $M(p;q)$ to be the maximum coefficient (in absolute value) that occurs in the family (1), thus $M(p;q) = \max\{A(pqr) : r > q\}$, with $2 < p < q$ fixed primes.

`Example`. Bang [6] proved that $M(p) \le p - 1$. Since $a_{3\cdot 5\cdot 7}(7) = -2$ we infer that $M(3) = 2$. Using $a_{105}(7) = -2$ and $M(3) = 2$, we infer that $M(3;5) = 2$.

Let $\mathcal{A}(p;q) = \{a_{pqr}(k) | r > q,\ k \ge 0\}$ be the set of coefficients occurring in the polynomial family (1).

Proposition 1 *We have* $\mathcal{A}(p;q) = [-M(p;q), M(p;q)] \cap \mathbb{Z}$.

This shows the relevance of understanding $M(p;q)$. Let us first recall some known results concerning the related function $M(p)$. Here we know thanks to Bachman [1], who very slightly improved on an earlier result in [8], that $M(p) \le 3p/4$. In 1968 it was conjectured by Sister Marion Beiter [7] (see also [8]) that $M(p) \le (p+1)/2$. She proved it for $p \le 5$. Since Möller [22] proved that $M(p) \ge (p+1)/2$ for $p > 2$, her conjecture actually would imply that $M(p) = (p+1)/2$ for $p > 2$. The first to show that Beiter's conjecture is false seems to have been Eli Leher (in his PhD thesis), who gave the counter-example $a_{17\cdot 29\cdot 41}(4801) = -10$, showing that $M(17) \ge 10 > 9 = (17+1)/2$. Gallot and Moree [15] provided for each $p \ge 11$ infinitely many infinitely many counter-examples $p \cdot q_j \cdot r_j$ with q_j strictly increasing with j. Moreover, they have shown that for every $\epsilon > 0$ and p sufficiently large $M(p) > (\frac{2}{3} - \epsilon)p$. They also proposed the Corrected Beiter Conjecture: $M(p) \le 2p/3$. The implications of their work for $M(p;q)$ are described in Section 4.

Proposition 1 together with Möller's result quoted above gives a different proof of the result, due to Bachman [2], that $\{a_{pqr}(k) |\ p < q < r\} = \mathbb{Z}$. For references and further results in this direction (begun by I. Schur) see Fintzen [14].

Jia Zhao and Xianke Zhang [25] showed that $M(7) = 4$, thus establishing the Beiter Conjecture for $p = 7$. In a later paper they eastablished the Corrected Beiter Conjecture:

Theorem 1 Zhao and Zhang [26]. *We have* $M(p) \le 2p/3$.

This result together with some computer computation allows one to extend the list of exactly known values of $M(p)$ (see Table 1). For a given prime p by 'smallest n', we mean the smallest integer n satisfying $A(n) = M(p)$ and with p as its smallest prime divisor.

TABLE 1

p	$M(p)$	smallest n
3	2	$3 \cdot 5 \cdot 7$
5	3	$5 \cdot 7 \cdot 11$
7	4	$7 \cdot 17 \cdot 23$
11	7	$11 \cdot 19 \cdot 601$
13	8	$13 \cdot 73 \cdot 307$
19	12	$19 \cdot 53 \cdot 859$

It is not known whether there is a finite procedure to determine $M(p)$. On the other hand, it is not difficult to see that there is such a procedure for $M(p;q)$.

Proposition 2 *Given primes $2 < p < q$, there is a finite procedure to determine $M(p;q)$.*

Recall that a set S of primes is said to have *natural density* δ if the ratio

$$\lim_{x\to\infty} \frac{|\{p \le x : p \in S\}|}{\pi(x)} = \delta,$$

with $\pi(x)$ the number of primes $p \le x$. A further question that arises is how often the maximum value $M(p)$ is assumed. Here we have the following theorem.

Theorem 2 *Given primes $2 < p < q$, there exists a prime q_0 with $q_0 \equiv q (\mathrm{mod}\ p)$ and an integer d such that $M(p,q) \le M(p,q_0) = M(p,q')$ for every prime $q' \ge q_0$ satisfying $q' \equiv q_0 (\mathrm{mod}\ d \cdot p)$. In particular the set of primes q with $M(p;q) = M(p)$ has a subset having a positive natural density.*

A weaker result in this direction, namely that for a fixed prime $p \ge 11$, the set of primes q such that $M(p;q) > (p+1)/2$ has a subset of positive natural density, follows from the work of Gallot and Moree [15] (recall that $M(p) > (p+1)/2$ for $p \ge 11$).

Unfortunately, the proof of Theorem 2 gives a lower bound for the density that seems to be far removed from the true value. In this paper we present some constructions that allow one to obtain much better bounds for the density for small p. These results are subsumed in the following main result of the paper.

Theorem 3 *Let $2 < p \le 19$ be a prime with $p \ne 17$. Then the set of primes q such that $M(p;q) = M(p)$ has a subset having natural density $\delta(p)$ as given in the table below.*

TABLE 2

p	3	5	7	11	13	19
$\delta(p)$	1	1	1	2/5	1/12	1/9

Numerical experimentation suggests that the set of primes q such that $M(p;q) = M(p)$ has a natural density $\delta(p)$ as given in the above table, except when $p = 13$ in which case numerical experimentation suggests $\delta(13) = 1/3$.

In order to prove Theorem 3, we will use the following theorem dealing with $2 < p \le 7$.

Theorem 4 *For $2 < p \le 7$ and $q > p$ we have $M(p;q) = (p+1)/2$, except in the case $p = 7$, $q = 13$ where $M(7;13) = 3$.*

The fact that $M(7;13) = 3$ can be explained. Indeed, it turns out that if $ap+bq = 1$ for small (in absolute value) integers a and b, then $M(p;q)$ is small. For example, one has the following result.

Theorem 5 *If $p \ge 5$ and $2p-1$ is a prime, then $M(p;2p-1) = 3$.*

This result and similar ones are established in Section 10.

Our main conjecture on $M(p;q)$ is the following one.

Conjecture 1 *Given a prime p, there exists an integer d and a function $g : (\mathbb{Z}/d\mathbb{Z})^* \to \mathbb{Z}_{>0}$ such that for some $q_0 > d$ we have for every prime $q \geq q_0$ that $M(p;q) = g(\overline{q})$, where $1 \leq \overline{q} < d$ satisfies $q \equiv \overline{q} (\bmod d)$. The function g is symmetric, that is we have $g(\alpha) = g(d - \alpha)$.*

The smallest integer d with the above properties, if it exists, we call the *ternary conductor* $\mathfrak{f}_p$. The corresponding smallest choice of q_0 (obtained on setting $d = \mathfrak{f}_p$) we call the *ternary minimal prime*. For $p = 7$ we obtain, e.g., $\mathfrak{f}_7 = 1$ and $q_0 = 17$ (by Theorem 4). Note that once we know q_0 it is a finite computation to determine d and the function g. Theorem 4 can be used to obtain the $p \leq 7$ part of the following observation concerning the ternary conductor.

Proposition 3 *If $2 < p \leq 7$, then the ternary conductor exists and we have $\mathfrak{f}_p = 1$. If $p \geq 11$ and $\mathfrak{f}_p$ exists, then $p | \mathfrak{f}_p$.*

While Theorem 2 only says that the set of primes q with $M(p;q) = M(p)$ has a subset having a positive natural density, Conjecture 1 implies that the set actually has a natural density in $\mathbb{Q}_{>0}$ which can be easily explicitly computed assuming we know q_0. In order to establish this implication one can invoke a quantitative form of Dirichlet's prime number theorem to the effect that, for $(a, d) = 1$, we have, as x tends to infinity,

$$\sum_{p \leq x,\ p \equiv a (\bmod\ d)} 1 \sim \frac{x}{\varphi(d) \log x}. \tag{2}$$

This result implies that asymptotically the primes are equidistributed over the primitive congruence classes modulo d. (Recall that Dirichlet's prime number theorem, Dirichlet's theorem for short, says that each primitive residue class contains infinitely many primes.)

The main tool in this paper is Kaplan's lemma and is presented in Section 6. The material in that section (except for Lemma 8 which is new), is taken from [16]. As a demonstration of working with Kaplan's lemma two examples (with and without table) are given in Section 6.1. In [17], the full version of this paper, details of further proofs using Kaplan's lemma can be found. In the shorter version we have merely written 'Apply Kaplan's lemma'.

The above summary of results makes clear how limited presently our knowledge of $M(p;q)$ is. For the benefit of the interested reader we present a list of open problems in the final section.

2 Proof of two propositions and Theorem 2

Proof of Proposition 1. By the definiton of $M(p;q)$ we have

$$\mathcal{A}(p;q) \subseteq [-M(p;q), M(p;q)] \cap \mathbb{Z}.$$

Let $r > q$ be a prime such that $A(pqr) = M(p;q)$ and suppose w.l.o.g. that $a_{pqr}(k) = M(p;q)$. Gallot and Moree [16] showed that we have $|a_n(k) - a_n(k -$

$1)| \le 1$ for ternary n (see Bachman [4] and Bzdęga [11] for alternative proofs). Since $a_{pqr}(k) = 0$ for every k large enough, it then follows that $0, 1, \ldots, M(p;q)$ are in $\mathcal{A}(p;q)$. By a result of Kaplan [19] (see Zhao and Zhang [25] for a different proof), we can find a prime $s \equiv -r \pmod{pq}$ and an integer k_1 such that $a_{pqs}(k_1) = -M(p;q)$. By a similar arguments as above one then infers that $-M(p;q), -M(p;q)+1, \ldots, -1, 0$ are all in $\mathcal{A}(p;q)$. □

Proof of Proposition 2. Let $\mathcal{R}_{pq}$ be a set of primes, all exceeding q such that every primitive residue class modulo pq is represented. By [19, Theorem 2] we have $A(pqr) = A(pqs)$ if $s \equiv r \pmod{pq}$ with s, r both primes exceeding q and hence

$$M(p;q) = \max\{A(pqr) : r \in \mathcal{R}_{pq}\}.$$

Since the computation of $\mathcal{R}_{pq}$ and $A(pqr)$ is a finite one, the computation of $M(p;q)$ is also finite. □

The remainder of the section is devoted to the proof of Theorem 2.

For coprime positive (not necessary prime) integers p, q, r we define

$$\Phi'_{p,q,r}(x) = \frac{(x^{pqr}-1)(x^p-1)(x^q-1)(x^r-1)}{(x-1)(x^{pq}-1)(x^{pr}-1)(x^{qr}-1)} = \sum_{k=0}^{\infty} a'_{p,q,r}(k)x^k.$$

Here we do not assume $p < q < r$. Hence we have the symmetry $\Phi'_{p,q,r}(x) = \Phi'_{p,r,q}(x)$. A routine application of the the inclusion-exclusion principle to the roots of the factors shows that $\Phi'_{p,q,r}(x)$ is a polynomial. It is referred to as a ternary inclusion-exclusion polynomial. Inclusion-exclusion polynomials can be defined in great generality, and the reader is referred to Bachman [4] for an introductory discussion. He shows that such polynomials and thus $\Phi'_{p,q,r}(x)$ in particular, can be written as products of cyclotomic polynomials ([4, Theorem 2]).

Analogously to $A(pqr)$ and $M(p;q)$ we define the following quantities:

$$A'(p,q,r) = \max\{|a'_{p,q,r}(k)| : k \ge 0\}, M'(p;q) = \max\{A'(p,q,r) : r \ge 1\}$$

$$\text{and } M'(p) = \max\{M'(p;q) : q \ge 1\}.$$

We have $\Phi_{pqr}(x) = \Phi'_{p,q,r}(x)$ if p, q, r are distinct primes and hence $A(pqr) = A'(p,q,r)$ in this case.

Lemma 1 *For coprime positive (not necessary prime) integers p, q, r we have $A'(p,q,r_1) \le A'(p,q,r_2) \le A'(p,q,r_1)+1$ if $r_2 \equiv r_1 \pmod{pq}$ and $r_2 > r_1$.*

Proof. Note that $r_2 > \max\{p,q\}$. If $r_1 > \max\{p,q\}$, then Kaplan, cf. proof of Theorem 2 in [19], showed that $A'(p,q,r_1) = A'(p,q,r_2)$. In the remaining case $r_1 < \max\{p,q\}$, we have $A'(p,q,r_1) \le A'(p,q,r_2) \le A'(p,q,r_1)+1$ by the Theorem in [5]. □

In Bachman and Moree [5] it is remarked that $A'(p,q,r_2) = A'(p,q,r_1)+1$ can occur.

Lemma 2 *If p is a prime, then $M'(p) = M(p)$. If q is also a prime with $q > p$ then $M'(p;q) = M(p;q)$.*

Proof. Let $p < q$ be primes. Assume $M'(p;q) = A'(p,q,r)$, where r is not necessary a prime. By Dirichlet's theorem we can find a prime r' satisfying $r' \equiv r (\text{mod } pq)$ and $r' > \max(q,r)$. Therefore we have by Lemma 1:

$$M'(p;q) = A'(p,q,r) \leq A'(p,q,r') = A(p,q,r') \leq M(p;q).$$

Since obviously $M(p;q) \leq M'(p;q)$, we have $M'(p;q) = M(p;q)$.

Now let only p be a prime. Assume $M'(p) = A'(p,q,r)$, where q and r are not necessary primes. Again by Dirichlet's theorem we find a prime q' with $q' \equiv q (\text{mod } pr)$ and $q' > \max(p,q)$. Using Lemma 1 we have:

$$M'(p) = A'(p,q,r) \leq A'(p,q',r) \leq M'(p,q') = M(p,q') \leq M(p).$$

Since obviously $M(p) \leq M'(p)$, we have $M'(p) = M(p)$. $\square$

Proof of Theorem 2. We set $q_1 := q$. Let r_i be a positive integer satisfying $M'(p;q_i) = A'(p,q_i,r_i)$. Using Lemma 1 (note that $A'(p,q,r)$ is invariant under permutations of p,q and r) we deduce:

$$M'(p;q_1) = A'(p,q_1,r_1) \leq A'(p,q_2,r_1) \leq A'(p,q_2,r_2) = M'(p,q_2),$$

where $q_2 = q_1 + pr_1$. By the same argument the sequence $q_1, q_2, q_3, \ldots$ with $q_{i+1} = q_i + pr_i$ satisfies:

$$M'(p;q_1) \leq M'(p;q_2) \leq M'(p;q_3) \leq \ldots$$

Since $M'(p;q) \leq M'(p) = M(p)$ and by, e.g., Lemma 4, $M(p)$ is finite, there are only finitely many different values for $M'(p;q)$. Hence there is an index k such that $M'(p;q_k) = M'(p;q_{k+i})$ for all $i \geq 0$. That means:

$$M'(p;q_k) = A'(p,q_k,r_k) = A'(p,q_{k+1},r_k) = A'(p,q_{k+1},r_{k+1}) = M'(p,q_{k+1}),$$

and by induction $A'(p,q_{k+i},r_k) = A'(p,q_{k+i},r_{k+i})$. Therefore we can assume $r_{k+i} = r_k$ for $i \geq 0$. Then we have $q_{k+i} = q_k + i \cdot pr_k$. We set $q_0 := q_k$ and $d := r_k$. Certainly we have $q_0 \equiv q (\text{mod } p)$. Let $q' \geq q_0$ be a prime with $q' \equiv q_0 (\text{mod } d \cdot p)$. There must be an integer m such that $q' = q_{k+m}$. Since $M'(p;q) = M(p;q)$ by Lemma 2, we have:

$$M(p;q_1) \leq M(p;q_0) = M(p;q').$$

Applying this to $M(p;q_1)$ with $M(p;q_1) = M(p)$, where we have chosen q_1 such that $M(p;q_1) = M(p)$, we get infinitely many primes of the form $q_i = q_1 + i \cdot pr_1$ satisfying $M(p;q_i) = M(p)$. On invoking (2) with $a = q_1$ and $d = pr_1$ the proof is then completed. $\square$

3 The bounds of Bachman and Bzdęga

Let q^* and r^*, $0 < q^*, r^* < p$ be the inverses of q and r modulo p respectively. Set $a = \min(q^*, r^*, p-q^*, p-r^*)$. Put $b = \max(\min(q^*, p-q^*), \min(r^*, p-r^*))$. In the sequel we will use repeatedly that $b \geq a$. Bachman in 2003 [1] showed that

$$A(pqr) \leq \min\left(\frac{p-1}{2} + a, p-b\right). \tag{3}$$

This was more recently improved by Bzdęga [11] who showed that

$$A(pqr) \leq \min(2a+b, p-b). \tag{4}$$

It is not difficult to show that $\min(2a+b, p-b) \leq \min(\frac{p-1}{2} + a, p-b)$ and thus Bzdęga's bound is never worse than Bachman's and in practice often strict inequality holds.

Note that if $q \equiv \pm 1 (\bmod\ p)$, then (3) implies that $A(pqr) \leq (p+1)/2$, a result due to Sister Beiter [7] and, independently, Bloom [10].

We like to remark that Bachman and Bzdęga define b as follows:

$$b = \min(b_1, p-b_1),\ ab_1qr \equiv 1 (\bmod\ p),\ 0 < b_1 < p.$$

It is an easy exercise to see that our definition is equivalent with this one.

We will show that both (3) and (4) give rise to the same upper bound $f(q^*)$ for $M(p;q)$. Write $q^* \equiv j (\bmod\ p)$, $r^* \equiv k (\bmod\ p)$ with $1 \leq j, k \leq p-1$. Thus the right hand side of both (3) and (4) are functions of j and k, which we denote by $GB(j,k)$, respectively $BB(j,k)$. We have

$$BB(j,k) = \min(2a+b, p-b) \leq \min\left(\frac{p-1}{2} + a, p-b\right) = GB(j,k),$$

with $a = \min(j, k, p-j, p-k)$ and $b = \max(\min(j, p-j), \min(k, p-k))$.

Lemma 3 *Let $1 \leq j \leq p-1$. Denote $GB(j,j)$ by $f(j)$. We have*

$$\max_{1 \leq k \leq p-1} BB(j,k) = \max_{1 \leq k \leq p-1} GB(j,k) = f(j), \text{ with}$$

$$f(j) = \begin{cases} (p-1)/2 + j & \text{if } j < p/4; \\ p-j & \text{if } p/4 < j \leq (p-1)/2, \end{cases}$$

and $f(p-j) = f(j)$ if $j > (p-1)/2$.

Proof. Since the problem is symmetric under replacing j by $p-j$, w.l.o.g. we may assume that $j \leq (p-1)/2$. If $j < p/4$, then

$$GB(j,k) \leq \frac{p-1}{2} + a \leq \frac{p-1}{2} + j = GB(j,j).$$

If $j > p/4$, then

$$GB(j,k) \leq p-b \leq p-j = GB(j,j).$$

Note that

$$GB(j,j) = \begin{cases} BB(j, \frac{p+1}{2} - j) & \text{if } j < p/4; \\ BB(j,j) & \text{if } j > p/4. \end{cases}$$

(E.g., if $j < p/4$, then the choice $q^* = j$, $r^* = (p+1)/2 - j$ leads to $a = j$ and $b = (p+1)/2 - j$ and hence $BB(j, (p+1)/2 - j) = \min((p+1)/2 + j, (p-1)/2 + j) = GB(j,j)$.) Since $BB(j,k) \le GB(j,k) \le GB(j,j)$ we are done. □

Theorem 6 *Let* $2 < p < q$. *Then* $M(p;q) \le f(q^*)$.

Proof. By (4) and the definition of $BB(j,k)$ we have

$$M(p;q) \le \max_{1 \le k \le p-1} BB(q^*, k) = f(q^*),$$

completing the proof. □

Lemma 3 shows that using either (3) or (4), we cannot improve on the upper bound given in Theorem 6. Since

$$\max_{1 \le j \le p-1} f(j) = p - 1 - \left[\frac{p}{4}\right] = \begin{cases} 3(p-1)/4 & \text{if } p \equiv 1 (\text{mod } 4); \\ (3p-1)/4 & \text{if } p \equiv 3 (\text{mod } 4), \end{cases}$$

we infer that

$$M(p) \le \max_{1 \le j \le p-1} \max_{1 \le k \le p-1} GB(j,k) = \max_{1 \le j \le p-1} f(j) < \frac{3}{4} p.$$

4 Earlier work on $M(p;q)$

Implicit in the literature are various results on $M(p;q)$ (although we are the first to explicitly study $M(p;q)$). Most of these are mentioned in the rest of this paper. Here we rewrite the main result of Gallot and Moree [15] in terms of $M(p;q)$ and use it for $p = 11$ and $p = 13$ (to deal with $q \equiv 4 (\text{mod } 11)$, respectively $q \equiv 5 (\text{mod } 13)$).

Theorem 7 *Let* $p \ge 11$ *be a prime. Given any* $1 \le \beta \le p-1$ *we let* β^* *be the unique integer* $1 \le \beta^* \le p-1$ *with* $\beta\beta^* \equiv 1 (\text{mod } p)$. *Let* $\mathcal{B}_-(p)$ *be the set of integers satisfying*

$$1 \le \beta \le \frac{p-3}{2},\ p \le \beta + 2\beta^* + 1,\ \beta > \beta^*.$$

Let $\mathcal{B}_+(p)$ *be the set of integers satisfying*

$$1 \le \beta \le \frac{p-3}{2},\ p \le \beta + \beta^*,\ \beta \ge \beta^*/2.$$

Let $\mathcal{B}(p)$ *be the union of these (disjoint) sets. As* $(p-3)/2 \in \mathcal{B}(p)$, *it is non-empty. Let* $q \equiv \beta (\text{mod } p)$ *be a prime satisfying* $q > p$. *Suppose that the inequality* $q > q_-(p) := p(p-\beta^*)(p-\beta^*-2)/(2\beta)$ *holds if* $\beta \in \mathcal{B}_-(p)$ *and*

$$q > q_+(p) := \frac{p(p-1-\beta)}{\gamma(p-1-\beta) - p + 1 + 2\beta},$$

with $\gamma = \min((p-\beta^*)/(p-\beta), (\beta^*-\beta)/\beta^*)$ *if* $\beta \in \mathcal{B}_+(p)$. *Then*

$$M(p;q) \geq p - \beta > \frac{p+1}{2}$$

and hence $M(p) \geq p - \min\{\mathcal{B}(p)\}$.

We have $\mathcal{B}(11) = \{4\}, \mathcal{B}(13) = \{5\}, \mathcal{B}(17) = \{7\}$ and $\mathcal{B}(19) = \{8\}$. In general one can show [12] using Kloosterman sum techniques that

$$\left||\mathcal{B}(p)| - \frac{p}{16}\right| \leq 8\sqrt{p}(\log p + 2)^3.$$

The lower bound for $M(p)$ resulting from this theorem, $p - \min\{\mathcal{B}(p)\}$, never exceeds $2p/3$ and this together with extensive numerical experimentation led Gallot and Moree [15] to propose the corrected Beiter conjecture, now proved by Zhao and Zhang (Theorem 1).

Under the appropriate conditions on p and q, Theorem 7 says that $M(p;q) \geq p - \beta$, whereas Theorem 6 yields $M(p;q) \leq f(\beta^*)$. Thus studying the case $p - \beta = f(\beta^*)$ with $\beta \in \mathcal{B}(p)$, leads to a small subset of cases where $M(p;q)$ can be exactly computed using Theorem 7.

Theorem 8 *Let* $p \geq 13$ *with* $p \equiv 1(\text{mod } 4)$ *be a prime. Let* x_0 *be the smallest positive integer such that* $x_0^2 + 1 \equiv 0(\text{mod } p)$. *If* $x_0 > p/3$, $q \equiv x_0(\text{mod } p)$ *and* $q \geq q_+(p)$ *(with* $\beta = x_0$*), then* $M(p;q) = p - x_0$.

Proof. Some easy computations show that if $p - \beta = f(\beta^*)$ and $\beta \in \mathcal{B}(p)$, we must have $\beta \in \mathcal{B}_+(p)$, $\frac{p-1}{2} < \beta^* < \frac{3}{4}p$ and hence $f(\beta^*) = \beta^*$ and so

$$\beta \in \mathcal{B}_+(p),\ 1 \leq \beta \leq \frac{p-3}{2},\ \beta + \beta^* = p,\ \beta^* \leq 2\beta,\ \frac{p-1}{2} < \beta^* < \frac{3}{4}p. \qquad (5)$$

Note that $\beta + \beta^* = p$, $p \geq 13$, has a solution with $\beta < p/2$ iff $p \equiv 1(\text{mod } 4)$ and $\beta = x_0$ (and hence $\beta^* = p - x_0$) with x_0 the smallest solution of $x_0^2 + 1 \equiv 0(\text{mod } p)$. If $x_0 > p/3$, then $\beta = x_0$ satisfies (5). Since by assumption $q \geq q_+(p)$ and $q \equiv x_0(\text{mod } p)$, we have $M(p;q) \geq p - x_0$ by Theorem 7. On the other hand, by Theorem 6, we have $M(p;q) \leq f(p - x_0) = f(x_0) = p - x_0$. □

`Remark`. The set of primes p satisfying $p \equiv 1(\text{mod } 4)$ and $x_0 > p/3$ (which starts $\{13, 29, 53, 73, 89, 173, \cdots\}$) has natural density 1/6. This follows on taking $\alpha_2 = 1/2$ and $\alpha_1 = 1/3$ in the result of Duke et al. [13], that if f is a quadratic polynomial with complex roots and $0 \leq \alpha_1 < \alpha_2 \leq 1$ are prescribed real numbers, then as x tends to infinity,

$$\#\{(p,v) : p \leq x,\ f(v) \equiv 0(\text{mod } p),\ \alpha_1 \leq \frac{v}{p} < \alpha_2\} \sim (\alpha_2 - \alpha_1)\pi(x).$$

5 Computation of $M(3;q)$

Note that for all primes q and r with $1 < q < r$, there exists some unique $h \leq (q-1)/2$ and $k > 0$ such that $r = (kq+1)/h$ or $r = (kq-1)/h$. If $n \equiv 0(\text{mod } 3)$ is ternary, then either $A(n) = 1$ or $A(n) = 2$ as $M(3) = 2$. The following result due to Sister Beiter [9] allows one to compute $A(n)$ in this case.

Theorem 9 *Let $n \equiv 0 (\text{mod } 3)$ be ternary.*
If $h = 1$, then $A(n) = 1$ iff $k \equiv 0 (\text{mod } 3)$.
If $h > 1$, then $A(n) = 1$ iff one of the following conditions holds:
(a) *$k \equiv 0 (\text{mod } 3)$ and $h + q \equiv 0 (\text{mod } 3)$.*
(b) *$k \equiv 0 (\text{mod } 3)$ and $h + r \equiv 0 (\text{mod } 3)$.*

We have seen that $M(3; 5) = 2$. The next result extends this.

Theorem 10 *Let $q > 3$ be a prime. We have $M(3; q) = 2$.*

Proof. In case $q \equiv 1 (\text{mod } 3)$, then let r be a prime such that $r \equiv 1 + q (\text{mod } 3q)$. Since $(1 + q, 3q) = 1$, there are in fact infinitely many such primes (by Dirichlet's theorem). In case $q \equiv 2 (\text{mod } 3)$, then let r be a prime such that $r \equiv 1 + 2q (\text{mod } 3q)$. Since $(1 + 2q, 3q) = 1$, there are infinitely many such primes. The prime r was chosen so to ensure that $h = 1$ and $3 \nmid k$. Using Theorem 9 it then follows that $A(3qr) = 2$ and hence $M(3; q) = 2$. □

6 Kaplan's lemma reconsidered

Our main tool will be the following recent result due to Kaplan [19], the proof of which uses the identity

$$\Phi_{pqr}(x) = (1 + x^{pq} + x^{2pq} + \cdots)(1 + x + \cdots + x^{p-1} - x^q - \cdots - x^{q+p-1})\Phi_{pq}(x^r).$$

Lemma 4 (Nathan Kaplan, 2007). *Let $2 < p < q < r$ be primes and $k \geq 0$ be an integer. Put*

$$b_i = \begin{cases} a_{pq}(i) & \text{if } ri \leq k; \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$a_{pqr}(k) = \sum_{m=0}^{p-1} (b_{f(m)} - b_{f(m+q)}), \tag{6}$$

where $f(m)$ is the unique integer such that $f(m) \equiv r^{-1}(k - m) (\text{mod } pq)$ and $0 \leq f(m) < pq$.

(If we need to stress the k-dependence of $f(m)$, we will write $f_k(m)$ instead of $f(m)$, see, e.g., Lemma 8 and its proof.) This lemma reduces the computation of $a_{pqr}(k)$ to that of $a_{pq}(i)$ for various i. These binary cyclotomic polynomial coefficients are computed in the following lemma. For a proof see, e.g., Lam and Leung [20] or Thangadurai [24].

Lemma 5 *Let $p < q$ be odd primes. Let ρ and σ be the (unique) non-negative integers for which $1 + pq = (\rho + 1)p + (\sigma + 1)q$. Let $0 \leq m < pq$. Then either $m = \alpha_1 p + \beta_1 q$ or $m = \alpha_1 p + \beta_1 q - pq$ with $0 \leq \alpha_1 \leq q - 1$ the unique integer*

such that $\alpha_1 p \equiv m(\text{mod } q)$ *and* $0 \le \beta_1 \le p-1$ *the unique integer such that* $\beta_1 q \equiv m(\text{mod } p)$. *The cyclotomic coefficient* $a_{pq}(m)$ *equals*

$$\begin{cases} 1 & \textit{if } m = \alpha_1 p + \beta_1 q \textit{ with } 0 \le \alpha_1 \le \rho,\ 0 \le \beta_1 \le \sigma; \\ -1 & \textit{if } m = \alpha_1 p + \beta_1 q - pq \textit{ with } \rho+1 \le \alpha_1 \le q-1,\ \sigma+1 \le \beta_1 \le p-1; \\ 0 & \textit{otherwise.} \end{cases}$$

We say that $[m]_p = \alpha_1$ is the *p-part of* m and $[m]_q = \beta_1$ is the *q-part of* m. It is easy to see that

$$m = \begin{cases} [m]_p p + [m]_q q & \text{if } [m]_p \le \rho \text{ and } [m]_q \le \sigma; \\ [m]_p p + [m]_q q - pq & \text{if } [m]_p > \rho \text{ and } [m]_q > \sigma; \\ [m]_p p + [m]_q q - \delta_m pq & \text{otherwise,} \end{cases}$$

with $\delta_m \in \{0, 1\}$. Using this observation we find that, for $i < pq$,

$$b_i = \begin{cases} 1 & \text{if } [i]_p \le \rho, [i]_q \le \sigma \text{ and } [i]_p p + [i]_q q \le k/r; \\ -1 & \text{if } [i]_p > \rho, [i]_q > \sigma \text{ and } [i]_p p + [i]_q q - pq \le k/r; \\ 0 & \text{otherwise.} \end{cases}$$

Thus in order to evaluate $a_{pqr}(n)$ using Kaplan's lemma it suffices to compute $[f(m)]_p$, $[f(m)]_q$, and $[f(m+q)]_q$ (note that $[f(m)]_p = [f(m+q)]_p$).

For future reference we provide a version of Kaplan's lemma in which the computation of b_i has been made explicit, and thus is self-contained.

Lemma 6 *Let* $2 < p < q < r$ *be primes and* $k \ge 0$ *be an integer. We put* $\rho = [(p-1)(q-1)]_p$ *and* $\sigma = [(p-1)(q-1)]_q$. *Furthermore, we put*

$$b_i = \begin{cases} 1 & \textit{if } [i]_p \le \rho, [i]_q \le \sigma \textit{ and } [i]_p p + [i]_q q \le k/r; \\ -1 & \textit{if } [i]_p > \rho, [i]_q > \sigma \textit{ and } [i]_p p + [i]_q q - pq \le k/r; \\ 0 & \textit{otherwise.} \end{cases}$$

We have

$$a_{pqr}(k) = \sum_{m=0}^{p-1} (b_{f(m)} - b_{f(m+q)}), \tag{7}$$

where $f(m)$ *is the unique integer such that* $f(m) \equiv r^{-1}(k-m)(\text{mod } pq)$ *and* $0 \le f(m) < pq$.

Note that if i and j have the same p-part, then $b_i b_j \ne -1$, that is b_i and b_j cannot be of opposite sign. From this it follows that $|b_{f(m)} - b_{f(m+q)}| \le 1$, and thus we infer from Kaplan's lemma that $|a_{pqr}(k)| \le p$ and hence $M(p) \le p$.

Using the mutual coprimality of p, q and r we arrive at the following trivial, but useful, lemma.

Lemma 7 *We have* $\{[f(m)]_q : 0 \le m \le p-1\} = \{0, 1, 2, \ldots, p-1\}$ *and* $|\{[f(m)]_p : 0 \le m \le p-1\}| = p$. *The same conclusions hold if we replace* $[f(m)]_q$ *and* $[f(m)]_p$ *by* $[f(m+q)]_q$, *respectively* $[f(m+q)]_p$.

On working with Kaplan's lemma one first computes $a_{pq}(f(m))$ and then $b_{f(m)}$. As a check on the correctness of the computations we note that the following identity should be satisfied.

Lemma 8 *We have*

$$\sum_{m=0}^{p-1} a_{pq}(f_k(m)) = \sum_{m=0}^{p-1} a_{pq}(f_k(m+q)).$$

Proof. Choose an integer $k_1 \equiv k (\text{mod } pq)$ such that $k_1 > pqr$. Then $a_{pqr}(k_1) = 0$. By Lemma 4 we find that

$$0 = a_{pqr}(k_1) = \sum_{m=0}^{p-1} [a_{pq}(f_{k_1}(m)) - a_{pq}(f_{k_1}(m+q))].$$

Since $f_k(m)$ only depends on the congruence class of k modulo pq, $f_{k_1}(m) = f_k(m)$ and the result follows. □

6.1 Working with Kaplan's lemma: examples

In this section we carry out some sample computations using Kaplan's lemma. For more involved examples the reader is referred to [15].

We remark that the result that $a_n(k) = (p+1)/2$ in Lemma 9 is due to Herbert Möller [22]. The proof we give here of this is rather different. The foundation for Möller's result is due to Emma Lehmer [21], who already in 1936 had shown that $a_n(\frac{1}{2}(p-3)(qr+1)) = (p-1)/2$ with p, q, r and n satisfying the conditions of Lemma 9.

Lemma 9 *Let $p < q < r$ be primes satisfying*

$$p > 3,\ q \equiv 2 (\text{mod } p),\ r \equiv \frac{p-1}{2} (\text{mod } p),\ r \equiv \frac{q-1}{2} (\text{mod } q).$$

For $k = (p-1)(qr+1)/2$ we have $a_{pqr}(k) = (p+1)/2$.

Proof (taken from [16].) Using that $q \equiv 2 (\text{mod } p)$, we infer from $1+pq = (\rho+1)p + (\sigma+1)q$ that $\sigma = \frac{p-1}{2}$ and $(\rho+1)p = 1 + (\frac{p-1}{2})q$ (and hence $\rho = (p-1)(q-2)/(2p)$). On invoking the Chinese remainder theorem one checks that

$$-r^{-1} \equiv 2 \equiv -\left(\frac{q-2}{p}\right) p + q (\text{mod } pq). \tag{8}$$

Furthermore, writing $f(0)$ as a linear combination of p and q we see that

$$f(0) \equiv \frac{k}{r} \equiv \left(\frac{p-1}{2}\right) q + \frac{p-1}{2r} \equiv \left(\frac{p-1}{2}\right) q + 1 - p \equiv \rho p (\text{mod } pq). \tag{9}$$

Since $f(m) \equiv f(0) - \frac{m}{r} (\text{mod } pq)$ we find using (8), (9) and the observation that $\rho - m(q-2)/p \geq 0$ for $0 \leq m \leq (p-1)/2$, that $[f(m)]_p = \rho - m(q-2)/p \leq \rho$ and $[f(m)]_q = m \leq \sigma$ for $0 \leq m \leq (p-1)/2$. Since $[f(m)]_p p + [f(m)]_q q = \rho p + 2m \leq \rho p + p - 1 = [k/r]$, we deduce that $a_{pq}(f(m)) = b_{f(m)} = 1$ in this range (see also Table 3).

TABLE 3

m	$[f(m)]_p$	$[f(m)]_q$	$f(m)$	$a_{pq}(f(m))$	$b_{f(m)}$
0	ρ	0	ρp	1	1
1	$\rho-(q-2)/p$	1	$\rho p+2$	1	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	1	1
j	$\rho-j(q-2)/p$	j	$\rho p+2j$	1	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	1	1
$(p-1)/2$	0	$(p-1)/2$	$(p-1)q/2$	1	1

Note that $f(m) \equiv f(0)-m/r \equiv \rho p+2m(\mathrm{mod}\ pq)$, from which one easily infers that $f(m)=\rho p+2m$ for $0 \le m \le p-1$ (as $\rho p+2m \le \rho p+2(p-1) < pq$). In the range $\frac{p+1}{2} \le m \le p-1$ we have $f(m) \ge \rho p+p+1=(p-1)q/2+2 > k/r$, and hence $b_{f(m)}=0$.

On noting that $f(m+q) \equiv f(m)-q/r \equiv f(m)+2q \equiv \rho p+2m+2q(\mathrm{mod}\ pq)$, one easily finds, for $0 \le m \le p-1$, that $f(m+q)=\rho p+2m+2q > k/r$ and hence $b_{f(m+q)}=0$.

On invoking Kaplan's lemma one finds

$$a_{pqr}(k)=\sum_{m=0}^{p-1} b_{f(m)}-\sum_{m=0}^{p-1} b_{f(m+q)}=\frac{p+1}{2}-0=\frac{p+1}{2}.$$

This concludes the proof. □

Lemma 10 *Let $3 < p < q < r$ be primes satisfying*

$$q \equiv 1(\mathrm{mod}\ p),\ r^{-1} \equiv \frac{p+q}{2}(\mathrm{mod}\ pq).$$

For $k=(p-1)qr/2-pr+2$ we have $a_{pqr}(k)=-\min(\frac{q-1}{p}+1,\frac{p+1}{2})$.

Proof. Let $0 \le m \le p-1$. We have:

$$\rho=\frac{(p-1)(q-1)}{p} \text{ and } \sigma=0,$$

$$k \equiv 1(\mathrm{mod}\ p),\ k \equiv 0(\mathrm{mod}\ q),\ k \equiv 2(\mathrm{mod}\ r),$$

so that we can compute:

$$[f(m)]_q \equiv q^{-1}r^{-1}(k-m) \equiv (1-m)/2(\mathrm{mod}\ p)$$

$$[f(m+q)]_q \equiv q^{-1}r^{-1}(k-m-q) \equiv -m/2(\mathrm{mod}\ p)$$

$$[f(m)]_p=[f(m+q)]_p \equiv p^{-1}r^{-1}(k-m) \equiv -m/2(\mathrm{mod}\ q).$$

This leads to:

$$[f(m)]_q=\begin{cases}(p+1-m)/2 & \text{for } m \text{ even}\\ (2p+1-m)/2 & \text{for } m \text{ odd and } m \neq 1\\ 0 & \text{for } m=1\end{cases}$$

$$[f(m+q)]_q = \begin{cases} (p-m)/2 & \text{for } m \text{ odd} \\ (2p-m)/2 & \text{for } m \text{ even and } m \neq 0 \\ 0 & \text{for } m = 0 \end{cases}$$

$$[f(m)]_p = [f(m+q)]_p = \begin{cases} (q-m)/2 & \text{for } m \text{ odd} \\ (2q-m)/2 & \text{for } m \text{ even and } m \neq 0 \\ 0 & \text{for } m = 0. \end{cases}$$

We consider the following four cases:

- Case 1: $[f(m)]_p \leq \rho$, $[f(m)]_q \leq \sigma$. In this case $m = 1$. Therefore:

$$[f(m)]_p p + [f(m)]_q q = \frac{p(q-1)}{2} > \frac{k}{r}.$$

- Case 2: $[f(m)]_p > \rho$, $[f(m)]_q > \sigma$. This case only arises if m is even and $m \geq 2$. Then we have:

$$[f(m)]_p p + [f(m)]_q q - pq = \frac{2q-m}{2}p + \frac{p+1-m}{2}q - pq$$

$$= \frac{q(p+1-m) - mp}{2} \leq \frac{q(p-1)}{2} - p + \frac{2}{r} = \frac{k}{r}.$$

  However, not all even $m \geq 2$ satisfy $[f(m)]_p > \rho$. For this it is necessary that $\frac{2q-m}{2} > \frac{(p-1)(q-1)}{p}$. That means $\frac{m}{2} < \frac{q-1}{p} + 1$ and by $0 < \frac{m}{2} \leq \frac{p-1}{2}$ we have exactly $\min(\frac{q-1}{p}, \frac{p-1}{2})$ different values of m in this case.

- Case 3: $[f(m+q)]_p \leq \rho$, $[f(m+q)]_q \leq \sigma$. In this case we have $m = 0$. Therefore:

$$[f(m+q)]_p p + [f(m+q)]_q q = 0 \leq \frac{k}{r}.$$

- Case 4: $[f(m+q)]_p > \rho$, $[f(m+q)]_q > \sigma$. We must have $2|m$ and $m \geq 2$. We find:

$$[f(m+q)]_p p + [f(m+q)]_q q - pq = \frac{2q-m}{2}p + \frac{2p-m}{2}q - pq > \frac{k}{r}.$$

The above case analysis shows that (respectively),

$$\sum_{\substack{m=0 \\ b_{f(m)}=1}}^{p-1} 1 = 0, \quad \sum_{\substack{m=0 \\ b_{f(m)}=-1}}^{p-1} 1 = \min\left(\frac{q-1}{p}, \frac{p-1}{2}\right), \quad \sum_{\substack{m=0 \\ b_{f(m+q)}=1}}^{p-1} 1 = 1, \quad \sum_{\substack{m=0 \\ b_{f(m+q)}=-1}}^{p-1} 1 = 0.$$

Kaplan's lemma then yields

$$a_{pqr}(k) = \left(0 - \min\left(\frac{q-1}{p}, \frac{p-1}{2}\right)\right) - (1-0) = -\min\left(\frac{q-1}{p} + 1, \frac{p+1}{2}\right).$$

Lemma 11 *Let $3 < p < q < r$ be primes satisfying*

$$q \equiv -2 (\mathrm{mod}\ p),\ \ r^{-1} \equiv p-2 (\mathrm{mod}\ pq)\ \text{ and } q > p^2/2.$$

For $k = \frac{p+1}{2}(1 + r(2-p+q)) + r + q - rq$ we have $a_{pqr}(k) = -(p+1)/2$.

Proof of Lemma 11. Apply Kaplan's lemma. □

`Remark`. Numerical experimentation suggests that with this choice of k, a condition of the form $q > p^2 c_1$, with c_1 some absolute positive constant, is unavoidable.

Lemma 12 *Let $3 < p < q < r$ be primes satisfying*

$$q \equiv -1 (\mathrm{mod}\ p),\ \ r^{-1} \equiv \frac{p+q}{2} (\mathrm{mod}\ pq)\ \text{ and } q \geq p^2 - 2p.$$

For $k = p(q-1)r/2 - rq + p - 1$ we have $a_{pqr}(k) = -(p+1)/2$.

Proof. Apply Kaplan's lemma. □

Proof of Proposition 3. The first assertion follows by Theorem 4, so assume $p \geq 11$. We will argue by contradiction. So suppose that $p \nmid \mathfrak{f}_p$. Put $\beta = (p-3)/2$. By the Chinese remainder theorem and Dirichlet's theorem there are infinitely many primes q_1 such that $q_1 \equiv 2 (\mathrm{mod}\ p)$ and $q_1 \equiv 1 (\mathrm{mod}\ \mathfrak{f}_p)$. Further, there are infinitely many primes q_2 such that $q_2 \equiv \beta (\mathrm{mod}\ p)$ and $q_2 \equiv 1 (\mathrm{mod}\ \mathfrak{f}_p)$. By the definition of $\mathfrak{f}_p$ there exists an integer c such that $M(p;q) = c$ for all $q \equiv 1 (\mathrm{mod}\ \mathfrak{f}_p)$ that are large enough. However, by Lemma 9 we have $M(p;q_1) = (p+1)/2$ and by Theorem 7 (note that $\beta \in \mathcal{B}(p)$) we have $M(p;q_2) > (p+1)/2$ for all q_2 large enough. This contradiction shows that $p \nmid \mathfrak{f}_p$. □

The results from this section together with those from Section 3 allow one to establish the following theorem. In Section 10 we will discuss the sharpness of the lower bounds for q.

Theorem 11 *Let $2 < p < q$ be primes.*
(a) *If $q \equiv 2 (\mathrm{mod}\ p)$, then $M(p;q) = (p+1)/2$.*
(b) *If $q \equiv -2 (\mathrm{mod}\ p)$ and $q > p^2/2$, then $M(p;q) = (p+1)/2$.*
(c) *If $q \equiv 1 (\mathrm{mod}\ p)$ and $q \geq (p-1)p/2 + 1$, then $M(p;q) = (p+1)/2$.*
(d) *If $q \equiv -1 (\mathrm{mod}\ p)$ and $q \geq p^2 - 2p$, then $M(p;q) = (p+1)/2$.*

Proof. By Theorem 10 we have $M(3;q) = 2 = (3+1)/2$, so assume $p > 3$.
(a) We have $M(p;q) \geq (p+1)/2$ by Lemma 9, and $M(p;q) \leq f(2^*) = f((p+1)/2) = (p+1)/2$ by Theorem 6.
(b)+(c)+(d) Similar to that of part (a). Note that $f((-2)^*) = f((p-1)/2) = (p+1)/2$ and $f(1) = f(p-1) = (p+1)/2$. □

Using Theorem 11 it is easy to establish the following result.

Theorem 12 *Let $q > 5$ be a prime. Then $M(5;q) = 3$.*

Proof. The proof is most compactly given by Table 4.

TABLE 4

$\overline{q}$	q_0	$M(5;q)$	result
1	11	3	Theorem 11 (c)
2	7	3	Theorem 11 (a)
3	13	3	Theorem 11 (b)
4	19	3	Theorem 11 (d)

The table should be read as follows. From, e.g., the third row we read that for $q \equiv 3(\text{mod } 5)$, $q \geq 13$, we have that $M(5;q) = 3$ by Theorem 11 (b). □

7 Computation of $M(7;q)$

Theorem 11 in addition with the following two lemmas allows one to compute $M(7;q)$. These lemmas concern the computation of $M(p;q)$ with $q \equiv (p \pm 1)/2(\text{mod } p)$.

Lemma 13 *Let $p \geq 5$ be a prime. Let $q \geq \max(3p, p(p+1)/4)$ be a prime satisfying $q \equiv \frac{p-1}{2}(\text{mod } p)$. Let $r > q$ be a prime satisfying*

$$r^{-1} \equiv \frac{p+1}{2}(\text{mod } p),\ r^{-1} \equiv p(\text{mod } q).$$

For $k = p - 1 + r(1 + q(p-1)/2 - p(p+1)/2)$ we have $a_{pqr}(k) = (p+1)/2$.

Proof. Apply Kaplan's lemma. □

Lemma 14 *Let $p \geq 5$ be a prime. Let $q \geq \max(3p, p(p-1)/4 + 1)$ be a prime satisfying $q \equiv \frac{p+1}{2}(\text{mod } p)$. Let $r > q$ be a prime satisfying*

$$r^{-1} \equiv \frac{p-1}{2}(\text{mod } p),\ r^{-1} \equiv p(\text{mod } q).$$

For $k = q + p - 1 + r(q(p-1)/2 - p(p+1)/2)$ we have $a_{pqr}(k) = (p+1)/2$.

Proof. Apply Kaplan's lemma. □

Theorem 13
(a) *Let $q \geq \max(3p, p(p+1)/4)$ be a prime satisfying $q \equiv \frac{p-1}{2}(\text{mod } p)$, then $(p+1)/2 \leq M(p;q) \leq (p+3)/2$.*
(b) *Let $q \geq \max(3p, p(p-1)/4 + 1)$ be a prime satisfying $q \equiv \frac{p+1}{2}(\text{mod } p)$, then $(p+1)/2 \leq M(p;q) \leq (p+3)/2$.*

Proof. Follows on noting that

$$f\Big(\big(\frac{p+1}{2}\big)^*\Big) = f(2) = \frac{p+3}{2} = f(p-2) = f\Big(\big(\frac{p-1}{2}\big)^*\Big),$$

and combining Lemmas 13 and 14 with Theorem 6. □

Theorem 14 *We have $M(7;11) = 4$, $M(7;13) = 3$ and for $q \geq 17$ a prime, $M(7;q) = 4$.*

Proof. The proof is most compactly given by a table (Table 5). Recall that Zhao and Zhang [25] proved that $M(7) \leq 4$.

TABLE 5

$\overline{q}$	q_0	$M(7;q)$	result
1	29	4	Theorem 11 (c)
2	23	4	Theorem 11 (a)
3	31	4	Theorem 13 (a) $+M(7) \leq 4$
4	53	4	Theorem 13 (b) $+M(7) \leq 4$
5	47	4	Theorem 11 (b)
6	41	4	Theorem11 (d)

Since $M(7;11) = M(7;17) = M(7;19) = 4$ and $M(7;13) = 3$ (the only cases not covered in Table 5), the proof is completed. □

Proof of Theorem 4. Follows on combining Theorems 10, 12 and 14. □

8 Computation of $M(11;q)$

We have $M(11;q) \leq M(11) = 7$ (by Theorem 1 and Table 1). From [15] we recall the following result.

Theorem 15 *Let $q < r$ be primes such that $q \equiv 4 (\mathrm{mod}\ 11)$ and $r \equiv -3 (\mathrm{mod}\ 11)$. Let $1 \leq \alpha \leq q-1$ be the unique integer such that $11r\alpha \equiv 1 (\mathrm{mod}\ q)$. Suppose that $q/33 < \alpha \leq (3q-1)/77$, then $a_{11qr}(10 + (6q - 77\alpha)r) = -7$.*

Lemma 15 *Let q be a prime such that $q \equiv 4 (\mathrm{mod}\ 11)$. For $q > 37$, $M(11;q) = 7$, and $M(11;37) = 6$.*

Proof. By computation one finds that $M(11;37) = 6$. Now assume $q > 37$. Notice that it is enough to show that $M(11;q) \geq 7$. For $q \geq 191$ the interval $I(q) := (q/33, (3q-1)/77]$ has length exceeding 1 and so contains at least one integer α_1. Then by the Chinese remainder theorem and Dirichlet's theorem we can find a prime r_1 such that both $r_1 \equiv -3 (\mathrm{mod}\ 11)$ and $11r_1\alpha_1 \equiv 1 (\mathrm{mod}\ q)$. Then we invoke Theorem 15 with $r = r_1$ and $\alpha = \alpha_1$. It remains to deal with the primes 59 and 103. One checks that both intervals $I(59)$ and $I(103)$ contain an integer and so we can proceed as in the case $q \geq 191$ to conclude the proof. □

Lemma 16 *Let $p = 11$.*
(a) *For ≥ 133, $q \equiv 3 (\mathrm{mod}\ 11)$, $r^{-1} \equiv \frac{q-19}{2} (\mathrm{mod}\ pq)$ and $k = q + 7r\frac{(q-19)}{2}$ we have $a_{pqr}(k) = 7$.*
(b) *For $q \equiv 7 (\mathrm{mod}\ 11)$, $r^{-1} \equiv \frac{q+7}{2} (\mathrm{mod}\ pq)$ and $k = 6qr + 4$ we have $a_{pqr}(k) = 7$.*
(c) *For $q \equiv 8 (\mathrm{mod}\ 11)$, $r^{-1} \equiv \frac{q-3}{2} (\mathrm{mod}\ pq)$ and $k = 6qr + 4$ we have $a_{pqr}(k) = 7$.*

Proof. Apply Kaplan's lemma. □

Theorem 16 *For $q \geq 13$ we have*

$q(\text{mod } 11)$	1	2	3	4	5	6	7	8	9	10
$M(11;q)$	6	6	7	7	6,7	6,7	7	7	6	6

except when $q \in \{17, 23, 37, 43, 47\}$. We have $M(11;17) = 5$, $M(11;23) = 3$, $M(11;37) = 6$, $M(11;43) = 5$ and $M(11;47) = 6$.

`Remark 1.` If $q \equiv \pm 5(\text{mod } 11)$ and $q \geq 61$, then $M(p,q) \in \{6,7\}$. We believe that $M(p;q) = 6$.
`Remark 2.` By Corollary 1 and 2 following Theorem 18, one infers that $M(11;17) \leq 5$, $M(11;23) \leq 3$ and $M(11;43) \leq 5$.

Proof of Theorem 16. We can most compactly prove this with a table.

TABLE 6

$\overline{q}$	q_0	$M(11;q)$	result
1	67	6	Theorem 11 (c)
2	13	6	Theorem 11 (a)
3	157	7	Lemma 16 (a) $+M(11) \leq 7$
4	59	7	Lemma 15
5	71	6,7	Theorem 13 (a) $+M(11) \leq 7$
6	61	6,7	Theorem 13 (b) $+M(11) \leq 7$
7	29	7	Lemma 16 (b) $+M(11) \leq 7$
8	19	7	Lemma 16 (c) $+M(11) \leq 7$
9	97	6	Theorem 11 (b)
10	109	6	Theorem 11 (d)

On directly computing the values of $M(p;q)$ not covered by the table, the proof is completed. □

9 Computation for $p = 19$

By Theorem 1 we have $M(19) \leq 2 \cdot 19/3$ and hence $M(19) \leq 12$. By Theorem 7 we find that $M(19;q) \geq 11$ for every $q \equiv 8(\text{mod } 19)$ and $q \geq 179$ and hence $M(19) \geq 11$. Since $A(19 \cdot 53 \cdot 859) = 12$, it follows that $M(19) = 12$. The next result even shows that $M(19;q) = M(19)$ for a positive fraction of the primes.

Theorem 17 *We have $M(19) = 12$. Moreover, $M(19,q) = 12$ if $q \equiv \pm 4(\text{mod } 19)$, with $q > 23$. Furthermore, $M(19;23) = 11$.*

The proof is an almost direct consequence of the following lemma.

Lemma 17 *Put $p = 19$ and let $q \equiv \pm 4(\text{mod } 19)$ be a prime. Suppose there exists an integer a satysifying*

$$qa \equiv -1(\text{mod } 3) \text{ and } \frac{q}{6p} < a \leq \frac{5q-18}{6p}. \tag{10}$$

Let $r > q$ be a prime satisfying $r(q-ap) \equiv 3(\text{mod } pq)$. Then $a_{pqr}(7qr+q) = -12$, if $q \equiv -4(\text{mod } 19)$, and $a_{19qr}(7qr+r) = -12$ if $q \equiv 4(\text{mod } 19)$.

Proof. Apply Kaplan's lemma. □

Proof of Theorem 17. For $q > 90$ the interval in (10) is of length > 3 and so contains an integer a satisfying $qa \equiv -1 (\mathrm{mod}\ 3)$. It remains to deal with $q \in \{23, 53, 61\}$. Computation shows that $M(19; 23) = 11$. For $q = 53$ and $q = 61$ one finds an integer a satisfying condition (10). □

Proof of Theorem 3. By Theorem 7 and Dirichlet's theorem the claim follows for $p = 13$. Using Lemmas 15 and 16 the result follows for $p = 11$. On invoking Theorems 4 and 17, the proof is then completed. □

10 Small values of $M(p; q)$

Typically if $M(p; q)$ is constant for all q large enough with $q \equiv a (\mathrm{mod}\ d)$, then $M(p; q)$ assumes a smaller value for some small q in this progression. A (partial) explanation of this phenomenon is provided in this section. We will show that if $ap + bq = 1$ with a and b small in absolute value, then $M(p; q)$ is small. On the other hand we will show that $M(p; q)$ cannot be truly small.

Proposition 4 *Let $2 < p < q$ be odd primes. Then $M(p; q) \geq 2$.*

Proof. We say $\Phi_n(x)$ is flat if $A(n) = 1$. ChunGang Ji [18] proved that if $p < q < r$ are odd prime and $2r \equiv \pm 1 (\mathrm{mod}\ pq)$, then $\Phi_{pqr}(x)$ is flat iff $p = 3$ and $q \equiv 1 (\mathrm{mod}\ 3)$. It follows that $M(p; q) \geq 2$ for $p > 3$. Now invoke Theorem 10 to deal with the case $p = 3$. □

Theorem 18 *Let $2 < p < q$ be odd primes and ρ and σ be the (unique) non-negative integers for which $1 + pq = (\rho + 1)p + (\sigma + 1)q$. Then*

$$M(p; q) \leq \begin{cases} p + \rho - \sigma & \text{if } \rho \leq \sigma; \\ q + \sigma - \rho & \text{if } \rho > \sigma. \end{cases}$$

Corollary 1 *Let h, k be integers with $k > h$ and $q = (kp - 1)/h$ a prime. If $p \geq k + h$, then $M(p; q) \leq k + h$.*

Corollary 2 *Let h, k be integers with $k > h$ and $q = (kp + 1)/h$ a prime. If $p > h$ and $q > k + h$, then $M(p; q) \leq k + h$.*

Proof of Theorem 18. Let us assume that $\rho \leq \sigma$, the other case being similar. Using Lemma 7 and Lemma 5 we infer that the number of $0 \leq m \leq p - 1$ with $b_{f(m)} = 1$ is at most $\rho + 1$. Likewise the number of m with $b_{f(m+q)} = -1$ is at most $p - 1 - \sigma$. By Kaplan's lemma it then follows that $a_{pqr}(k) \leq \rho + 1 + (p - 1 - \sigma) = p + \rho - \sigma$. Since the number of $0 \leq m \leq p - 1$ with $b_{f(m)} = -1$ is at most $p - 1 - \sigma$ and the number of m with $b_{f(m+q)} = 1$ is at most $\rho + 1$, we infer that $a_{pqr}(k) \geq -(p + \rho - \sigma)$ and hence the result is proved. □

Theorem 19 *Let $q \equiv 1 (\mathrm{mod}\ p)$. Then*

$$M(p; q) = \min\Big(\frac{q - 1}{p} + 1, \frac{p + 1}{2}\Big).$$

Proof. For $p = 3$ the result follows by Theorem 10, so assume $p \geq 5$. Sister Beiter [7], and independently Bloom [10], proved that $M(p;q) \leq (p+1)/2$ if $q \equiv \pm 1(\text{mod } p)$ (alternatively we invoke Theorem 6). By Corollary 2 we have $M(p;q) \leq (q-1)/p + 1$. By Lemma 10 the proof is then completed. □

Numerical experimentation suggests that in part (b) of Theorem 11 perhaps the condition $q > p^2/2$ can be dropped. By Theorem 19 the condition $q \geq (p-1)p/2 + 1$ in part (c) is optimal. In part (d) we need $q \geq (p-1)p/2 - 1$, for otherwise $M(p;q) < (p+1)/2$ by Corollary 1.

Lemma 18 *Let $p \geq 7$ be a prime such that $q = 2p - 1$ is also a prime. Let $r > q$ be a prime such that $(p+q)r \equiv -2(\text{mod } pq)$. Put $k = rq(p-1)/2 + 2p - pq$. Then $a_{pqr}(k) = 3$.*

Proof. Apply Kaplan's lemma. □

Proof of Theorem 5. On combining Lemma 18 with Corollary 1, one deduces that $M(p; 2p-1) = 3$ if $p \geq 5$ and $2p - 1$ is a prime. □

11 Conjectures, questions, problems

The open problem that we think is the most interesting is Conjecture 1. Note that if one could prove Conjecture 1 and getting an effective upper bound for the ternary conductor $\mathfrak{f}_p$ (say $16p$) and an effective upper bound for the minimal ternary prime (say p^3), then one has a finite procedure to compute $M(p)$.

Problem 1 *Bachman* [4] *introduced inclusion-exclusion polynomials. These polynomials generalize the ternary cyclotomic polynomials. Study $M(p;q)$ in this setting (here p and q can be any coprime natural numbers), cf. Section 2 where we denoted this function by $M'(p;q)$. For example, using [4, Theorem 3] by an argument similar to that given in Proposition 2 it is easily seen that there is a finite procedure to compute $M'(p;q)$.*

Problem 2 *The analogue of $M(p;q)$ for inverse cyclotomic polynomials, see* [23], *can be defined. Study it.*

Question 1 *Can one compute the average value of $M(p;q)$, that is does the limit*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p<q\leq x} M(p;q)$$

exist and if yes, what is its value?

Question 2 *Is Theorem* 3 *still true if we put $\delta(13) = 1/3$ and cross out the words 'a subset having'?*

Question 3 *If $q > p$ is prime and $q \equiv -2(\text{mod } p)$, then do we have $M(p;q) = (p+1)/2$?*

Question 4 *Suppose that $p > 11$ is a prime.*
If $6p-1$ is prime, then do we have $M(p, 6p-1) = 7$?
If $(5p-1)/2$ is prime, then do we have $M(p,(5p-1)/2) = 7$?
If $(5p+1)/2$ is prime then do we have $M(p,(5p+1)/2) = 7$?
Find more similar results.

Question 5 *Given an integer $k \geq 1$, does there exist $p_0(k)$ and a function $q_k(p)$ such that if $q \equiv 2/(2k+1) (\mathrm{mod}\ p)$, $q \geq q_k(p)$ and $p \geq p_0(k)$, then $M(p;q) = (p+2k+1)/2$?*

Question 6 *Is it true that $M(11;q) = 6$ for all large enough q satisfying $q \equiv \pm 5 (\mathrm{mod}\ 11)$? If so one can finish the computation of $M(11;q)$.*

Question 7 *Is it true that for q sufficiently large the values of $M(13;q)$, $M(17;q)$, $M(19;q)$ and $M(23;q)$ are given by the following tables?*

$q(\mathrm{mod}\ 13)$	1	2	3	4	5	6	7	8	9	10	11	12
$M(13;q)$	7	7	7	8	8	7	7	8	8	7	7	7

$q(\mathrm{mod}\ 17)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$M(17;q)$	9	9	9	10	10	9	10	9	9	10	9	10	10	9	9	9

$q(\mathrm{mod}\ 19)$	1	2	3	4	5	6	7	8	9
$M(19;q)$	10	10	10	12	11	9	11	11	10
$q(\mathrm{mod}\ 19)$	10	11	12	13	14	15	16	17	18
$M(19;q)$	10	11	11	9	11	12	10	10	10

$q(\mathrm{mod}\ 23)$	1	2	3	4	5	6	7	8	9	10	11
$M(23;q)$	12	12	12	14	14	11	13	11	14	13	12
$q(\mathrm{mod}\ 23)$	12	13	14	15	16	17	18	19	20	21	22
$M(23;q)$	12	13	14	11	13	11	14	14	12	12	12

The next question is raised by the referee of this paper.

Question 8 *Suppose that for all sufficiently large primes $q \equiv q_0 (\mathrm{mod}\ \mathfrak{f}_p)$ we have $M(p;q) < M(p)$. Is it possible to prove that $M(p;q) < M(p)$ for every prime $q \equiv q_0 (\mathrm{mod}\ \mathfrak{f}_p)$?*

Question 9 *For a given prime p, let $m(p)$ denote $\liminf M(p;q)$, with $q > p$. Determine $m(p)$. Is it true that $\lim_{p\to\infty} m(p)/p = c$ for some constant $c > 0$?*

By Proposition 4 we have $m(p) \geq 2$ for $p > 2$. Note that the results in this paper imply that $m(p) = (p+1)/2$ for $2 < p \leq 11$. If the answer to Question 7 is yes, then $m(p) = (p+1)/2$ for $2 < p \leq 17$ and $m(p) = (p-1)/2$ for $19 \leq p \leq 23$. (The issue of lower bounds for $M(p;q)$ was raised by the referee.)

`Acknowledgement`. The second author likes to thank the MPIM interns (in June 2008) N. Baghina, C. Budde, B. Jüttner and D. Sullivan for their (computer) assistance in computing tables used in the proofs of Lemma 17 ($p = 19$). For

these tables see [17]. However, the bulk of the paper was written whilst the third author was during two months in 2010 an intern at MPIM under the guidance of the second author. The third author would like to thank the MPIM for the possibility to do an internship and for the nice research atmosphere. He also thanks the second author for his mentoring and for having a sympathetic ear for any questions.

Finally thanks are due to G. Bachman for some helpful remarks, and the referee who spent quite a bit of time writing a very extensive referee report, which led to many improvements over the original submission.

References

[1] G. Bachman, On the coefficients of ternary cyclotomic polynomials, *J. Number Theory* **100** (2003), 104–116.

[2] G. Bachman, Ternary cyclotomic polynomials with an optimally large set of coefficients, *Proc. Amer. Math. Soc.* **132** (2004), 1943–1950.

[3] G. Bachman, Flat cyclotomic polynomials of order three, *Bull. London Math. Soc.* **38** (2006), 53–60.

[4] G. Bachman, On ternary inclusion-exclusion polynomials, *Integers* **10** (2010), A48, 623–638.

[5] G. Bachman and P. Moree, On a class of ternary inclusion-exclusion polynomials, *Integers* **11** (2011), A8, 14 pp.

[6] A.S. Bang, Om Ligningen $\varphi_n(x) = 0$, *Nyt Tidsskrift for Mathematik (B)* **6** (1895), 6–12.

[7] M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$, *Amer. Math. Monthly* **75** (1968), 370–372.

[8] M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}. II, *Duke Math. J.* **38** (1971), 591–594.

[9] M. Beiter, Coefficients of the cyclotomic polynomial $F_{3qr}(x)$, *Fibonacci Quart.* **16** (1978), 302–306.

[10] D.M. Bloom, On the coefficients of the cyclotomic polynomials, *Amer. Math. Monthly* **75** (1968), 372–377.

[11] B. Bzdęga, Bounds on ternary cyclotomic coefficients, *Acta Arith.* **144** (2010), 5-16.

[12] C. Cobeli, Y. Gallot and P. Moree, unpublished manuscript.

[13] W. Duke, J.B. Friedlander and H. Iwaniec, Equidistribution of roots of a quadratic congruence to prime moduli, *Ann. of Math.* (2) **141** (1995), 423–441.

[14] J. Fintzen, Cyclotomic polynomial coefficients $a(n, k)$ with n and k in prescribed residue classes, *J. Number Theory* **131** (2011), 1852–1863.

[15] Y. Gallot and P. Moree, Ternary cyclotomic polynomials having a large coefficient, *J. Reine Angew. Math.* **632** (2009), 105–125.

[16] Y. Gallot and P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, *J. Ramanujan Math. Soc.* **24** (2009), 235–248.

[17] Y. Gallot, P. Moree and R. Wilms, The family of ternary cyclotomic polynomials with one free prime, MPIM-preprint 2010-11, pp. 32.

[18] C. Ji, A specific family of cyclotomic polynomials of order three, *Sci. China Math.* **53** (2010), 2269–2274.

[19] N. Kaplan, Flat cyclotomic polynomials of order three, *J. Number Theory* **127** (2007), 118–126.

[20] T.Y. Lam and K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, *Amer. Math. Monthly* **103** (1996), 562–564.

[21] E. Lehmer, On the magnitude of the coefficients of the cyclotomic polynomials, *Bull. Amer. Math. Soc.* **42** (1936), 389–392.

[22] H. Möller, Über die Koeffizienten des n-ten Kreisteilungspolynoms, *Math. Z.* **119** (1971), 33–40.

[23] P. Moree, Inverse cyclotomic polynomials, *J. Number Theory* **129** (2009), 667–680.

[24] R. Thangadurai, On the coefficients of cyclotomic polynomials, *Cyclotomic fields and related topics* (Pune, 1999), 311–322, Bhaskaracharya Pratishthana, Pune, 2000.

[25] J. Zhao and X. Zhang, Coefficients of ternary cyclotomic polynomials, *J. Number Theory* **130** (2010), 2223-2237.

[26] J. Zhao and X. Zhang, A proof of the Corrected Beiter conjecture, arXiv:0910.2770.

12 bis rue Perrey, 31400 Toulouse, France.
e-mail: `galloty@orange.fr`

Max-Planck-Institut für Mathematik,
Vivatsgasse 7, D-53111 Bonn, Germany.
e-mail: `moree@mpim-bonn.mpg.de`

Sterbeckerstrasse 21, 58579 Schalksmühle, Germany
e-mail: `Robert.wilms@rub.de`